

USDC SDNY DOCUMENT ELECTRONICALLY FILED DOC #: DATE FILED: 5/5/2023

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

Google LLC,

Plaintiff,

-against-

Zubair Saeed; Raheel Arshad; Mohammad
Rasheed Siddiqui; and Does 1–15,

Defendants.

Civil Action No. 1:23-cv-03369-VEC

PRELIMINARY INJUNCTION ORDER

Plaintiff Google LLC has filed a complaint for injunctive and other relief to stop Defendants Zubair Saeed, Raheel Arshad, Mohammad Rasheed Siddiqui, and Does 1 through 15—through their participation in, and operation of, the Malware Distribution Enterprise—from continuing to distribute malware to infect new devices, control and operate a botnet, and carry out criminal schemes.

Google filed a complaint alleging claims under: (1) the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1962(c)-(2) (Count I); (2) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (Count II); (3) the Lanham Act, 15 U.S.C. § 1114 (Count III); the Lanham Act, 15 U.S.C. § 1125(a) (Count IV); and tortious interference with business relationships (Count V). On April 25, 2023, this Court issued a temporary restraining order for Defendants to show cause why a preliminary injunction should not issue. ECF No. 13.

THE COURT HEREBY FINDS THAT:

Jurisdiction and Venue

1. This Court has federal question jurisdiction over Google’s claims under RICO, the Computer Fraud and Abuse Act, and the Lanham Act under 28 U.S.C. § 1331. This Court

also has jurisdiction over the Lanham Act under 28 U.S.C. § 1338 and 15 U.S.C. § 1121. This Court has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

2. This Court has personal jurisdiction over the Defendants because:

- a. The Defendants distribute malware to Google users in this district and within New York State;
- b. The Defendants send commands to infected user computers in this district and within New York State to carry out their illicit schemes;
- c. Google's complaint and moving papers demonstrate that the Defendants undertook these activities intentionally and with knowledge that their actions would cause harm to users in New York and cause Google harm in New York. Google does business in New York and has done business in New York for many years.

3. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are not residents of the United States and may be sued in any judicial district. Venue is also proper in this judicial district under 28 U.S.C. § 1391(b) and 18 U.S.C. § 1965 because a substantial part of the events or omissions giving rise to Google's claims occurred in this judicial district, because a substantial part of the property that is the subject of Google's claims is situated in this judicial district, because a substantial part of the harm caused by Defendants has occurred in this judicial district, and because Defendants transact their affairs in this judicial district. Moreover, Defendants are subject to personal jurisdiction in this district and no other venue appears to be more appropriate.

4. The complaint pleads fact with the specificity required by the Federal Rules and states claims against Defendants for violations of (1) the Racketeer Influenced and Corrupt

Organizations Act, 18 U.S.C. §§ 1962(c)–(2) (Count I); (2) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (Count II); (3) the Lanham Act, 15 U.S.C. § 1114 (Count III); the Lanham Act, 15 U.S.C. § 1125(a) (Count IV); and tortious interference with business relationships (Count V).

Preliminary Injunction Order Factors

The Court finds that Google has established each of the factors required for preliminary injunction: (1) irreparable harm; (2) a likelihood of success on the merits or a substantial question as to the merits; (3) the balance of hardships tips in Google’s favor; and (4) a preliminary injunction serves the public interest. *Citigroup Glob. Markets, Inc. v. VCG Special Opportunities Master Fund Ltd.*, 598 F.3d 30, 34 (2d Cir. 2010); *see also AIM Int’l Trading, LLC v. Valcucine, SpA*, 188 F. Supp. 2d 384, 386 (S.D.N.Y. 2002) (same).

Irreparable Harm

5. Google has established that it will suffer immediate, irreparable harm if this Court denies its request for a preliminary injunction. In particular, it has shown that the Defendants—through their participation in, and operation of, the Malware Distribution Enterprise—have threatened the security of the Internet, including Google platforms, by transmitting malware through the Internet to configure, deploy, and operate a botnet, as well as to distribute cracked software. The Enterprise has distributed malware on devices of Google users, compromising the security of those devices and continues to issue commands to those devices to carry out criminal activities, such as selling access to Google user accounts.

6. The Defendants are responsible for distributing a botnet that has infected approximately 672,220 CryptBot victim devices in the U.S. in the last year. At any moment, the botnet’s extraordinary computing power could be harnessed for other criminal schemes. Defendants could, for example, enable large ransomware or distributed denial-of-service attacks

on legitimate businesses and other targets. Defendants could themselves perpetrate such a harmful attack, or they could sell access to the botnet to a third party for that purpose.

7. In addition, Defendants' conduct is infringing Google's trademarks, injuring Google's goodwill, and damaging its reputation by creating confusion as to the source of the CryptBot malware because Defendants infringe, among others, Google's Google Earth Pro and Google Chrome marks that are used to distribute cracked versions of those applications leading to the installation of malware. This constitutes irreparable harm.

Likelihood of Success on the Merits

8. Google has shown at a minimum that its complaint presents a substantial question as to each of its claims, and indeed that it is likely to succeed on the merits of its claims. *See Sterling v. Deutsche Bank Nat'l Tr. Co. as Trustees for Femit Tr. 2006-FF6*, 368 F. Supp. 3d 723, 727 (S.D.N.Y. 2019).

9. CFAA. Google has shown a likelihood of success on the merits of its claim that Defendants violated and continue to violate the Computer Fraud and Abuse Act. The CFAA prohibits, among other things, knowingly and with intent to defraud trafficking in any password or similar information through which a computer may be accessed without authorization if such trafficking affects interstate or foreign commerce. 18 U.S.C. § 1030(a)(6)(A). Defendants knowingly and with intent to defraud accessed users' computers operating in interstate commerce through the Internet, without authorization, to infect them with malware. They did so to obtain information such as account credentials, for the purposes of selling those credentials to others. This has affected well over ten computers within a one-year span and resulted in damages significantly in excess of \$5,000.

10. Lanham Act. Google has shown a likelihood of success on the merits of its claim that Defendants violated and continue to violate Sections 32 and 43(a) of the Lanham Act

because they have infringed and wrongfully used the Google Marks (as defined in ¶¶ 7–9 of the Complaint). See 15 U.S.C. §§ 1114, 1125(a). Google owns a number of federal registrations for the Google Marks used by the Defendants sufficient to show these are valid marks entitled to protection. Additionally, Defendants’ conduct in using copies, reproductions, and/or counterfeits of the Google Marks to distribute cracked versions of software further containing malware, including CryptBot, is likely to confuse or deceive users as to the origin or affiliation of the cracked software and malware within. By showing a likelihood of success on the merits of their Lanham Act claims, Google is also entitled to a presumption of irreparable harm. 15 U.S.C. § 1116(a).

11. RICO. Google has also shown a likelihood of success on the merits of its claims that Defendants have violated and continue to violate the RICO statute.

- a. Google has shown that each Defendant is an active participant in the distribution and operation of the CryptBot botnet as well as illegally cracked software, and leverage the Cracked Software Sites to distribute the botnet.
- b. Defendants Zahid Saeed, Raheel Arshad, and Mohammad Rasheed Siddiqui each manage and market one or more of the Cracked Software Sites.
- c. Defendants Zahid Saeed, Raheel Arshad, and Mohammad Rasheed Siddiqui are also all associated with the Cracked Software Sites’ primary web hosting company, known as Offshoric.
- d. Google has established that Defendants have formed an enterprise. Defendants share a common purpose to spread malware via cracked

software to build a botnet that is deployed for numerous criminal schemes for profit. Defendants work together to accomplish this purpose, each playing a role as described above.

- e. Google has established that Defendants have engaged in a pattern of racketeering activity. The predicate acts include a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A). Defendants have violated and will continue to violate the CFAA, resulting in damage as defined in § 1030(c)(4)(A)(i)(VI), by infecting computers with malware, transmitting to such protected computers programs designed to carry out their schemes, and transmitting to such protected computers commands to infected computers. For instance, Defendants have transmitted commands to protected computers through the Internet, thereby causing damage to those computers and enabling the Malware Distribution Enterprise to utilize these computers in its criminal schemes. Google is also likely to succeed on the merits of showing that the Defendants have committed predicate acts including violations of the federal wire fraud statute, 18 U.S.C. § 1343, federal identity fraud statute, 18 U.S.C. § 1028(a)(7), and federal access device fraud statute, 18 U.S.C. §§ 1029(a)(2), (3).
- f. Google has suffered injury to its business or property as a result of these predicate offenses.

12. Google has also shown a likelihood of success on the merits of its New York common law claim for tortious interference with business relationships.

Balance of the Hardships

13. The equities also favor a preliminary injunction. The criminal enterprise is defrauding users and injuring Google. There is no countervailing factor weighing against a preliminary injunction: there is no legitimate reason why Defendants should be permitted to continue to disseminate malware and cracked software and manipulate infected computers to carry out criminal schemes.

Public Interest

14. Google has shown that the public interest favors granting a preliminary injunction.

15. Every day that passes, the Defendants infect new computers, steal more account information, and deceive more unsuspecting victims. Protection from malicious cyberattacks and other cybercrimes is strongly in the public interest.

16. And the public interest is clearly served by enforcing statutes designed to protect the public, such as RICO, the CFAA, and the Lanham Act.

Good Cause for Alternative Service

17. The Court finds good cause continues to exist to grant alternative service of the filings in this matter via mail, email, text, and/or service through ICANN because Google establishes that traditional service methods would be futile. Given the online nature of Defendants' conduct, alternative service is most likely to give Defendants' notice of the filings pertaining to this lawsuit.

PRELIMINARY INJUNCTION ORDER

IT IS HEREBY ORDERED that Defendants, any of their officers, agents, servants, employees, attorneys, and all others in active concert or participation with them, who receive

actual notice of this Order by personal service or otherwise including email and text (“Restrained Parties”), are restrained and enjoined, from anywhere in the world:

1. Intentionally accessing and sending malicious code to the protected computers of Google’s customers, without authorization;
2. Intentionally designing malicious software to target Google Chrome and Google Chrome users;
3. Sending malicious code to configure, deploy, and operate a botnet;
4. Attacking and compromising the security of the computers and networks of Google’s users;
5. Stealing and exfiltrating information from computers and computer networks;
6. Creating websites that falsely indicate that they are associated with Google or any other Google affiliate, through use of the Google Marks and/or other false and/or misleading representations;
7. Creating or maintaining websites that advertise or distribute “pirated,” “cracked,” or otherwise altered versions of proprietary software, including but not limited to the websites associated with the domains listed in Appendix A to Google’s complaint;
8. Configuring, deploying, operating, or otherwise participating in or facilitating any botnet, including but not limited to the C2 servers hosted at and operating through the domains listed in Appendix B to Google’s complaint and through any other component or element of the botnet in any location;
9. Delivering malicious code designed to steal credentials and cookies;
10. Monitoring the activities of Google or Google’s users and stealing information from them;

11. Selling access to the accounts of Google's users;
12. Corrupting applications on victims' computers and networks, thereby using them to carry out the foregoing activities;
13. Misappropriating that which rightfully belongs to Google, Google's users, or in which Google has a proprietary interest; and
14. Using, linking to, transferring, selling, exercising control over, or otherwise owning or accessing the domains attached in Appendix A or Appendix B to the complaint;
15. Using, transferring, exercising control over, or accessing any accounts used in the transfer of money or electronic currency, including cryptocurrency, or in the processing of card-based transactions, as a means to further Defendants' unlawful schemes;
16. Undertaking any similar activity that inflicts harm on Google, Google's customers, or the public.

Upon service via mail, email, or text, the Defendants and other Restrained Parties shall be deemed to have actual notice of the issuance and terms of the preliminary injunction order, and by any of the Restrained Parties in violation of any of the terms of the preliminary injunction order may be considered and prosecuted as contempt of Court.

In the event Google identifies additional domains or individuals used in connection with Defendants' scheme, Google may move the Court for an order modifying this injunction as appropriate and may amend its complaint to include the additional parties.

IT IS FURTHER ORDERED that Defendants, their representatives and persons who are in active concert or participation with them are restrained and enjoined from, anywhere in the world:

1. Using and infringing the Google Marks, including specifically Google's Google Earth Pro and Google Chrome marks;
2. Using in connection with Defendants' activities, products or services with any false or deceptive designation, representations or descriptions of Defendants or any of their activities, whether by symbols, words, designs or statements, which would damage or injure Google or its users or give Defendants an unfair competitive advantage or result in deception of consumers; and
3. Acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Google, or passing off Defendants' activities, products or services as Google's.

IT IS FURTHER ORDERED that Google may serve this Order on the persons and entities providing services to the domains identified in Appendix A or Appendix B to the complaint, requesting that those persons and entities take reasonable best efforts to implement the following actions:

1. Take reasonable steps to identify incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the domains identified in Appendix A and/or Appendix B to the complaint;
2. Take reasonable steps to block incoming and/or outgoing Internet traffic on their respective networks that originate and/or are being sent from and/or to the domains identified in Appendix A and/or Appendix B to the complaint by Defendants or Defendants' representatives or resellers, except as explicitly provided for in this Order;

3. Take other reasonable steps to block such traffic to and/or from any other IP addresses or domains to which Defendants may move the botnet infrastructure, to ensure that Defendants cannot use such infrastructure to control the botnet;

4. Take other reasonable steps to block such traffic to and/or from any other IP addresses or domains to which Defendants use for websites distributing cracked or pirated software, to ensure Defendants cannot use such infrastructure to distribute malware;

5. Disable completely the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the domains set forth in Appendix A and/or Appendix B to the complaint and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives, and all other persons, except as otherwise ordered herein;

6. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with the domains set forth in Appendix A to the complaint;

7. Transfer any content and software hosted at the domains listed in Appendix A and/or Appendix B to the complaint that are not associated with Defendants, if any, to new domains not listed in Appendix A and/or Appendix B; notify any non-party owners of such action and the new domains, and direct them to contact Google's counsel, Andrew S. Pak at Perkins Coie LLP, 1155 Avenue of the Americas, 22nd Floor, New York, NY 10036-2711 to facilitate any follow-on action;

8. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until the

steps required by this Order are executed in full, except as necessary to communicate with hosting companies, data centers, Google, or other ISPs to execute this Order;

9. Not enable, and take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the domains, including without limitation to enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain other domains and IP addresses associated with your services;

10. Preserve, retain, and produce to Google all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the domains set forth in Appendix A and/or Appendix B to the complaint including any and all individual or entity names, mailing addresses, email addresses, facsimile numbers, telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with the use of or access to such domains;

11. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

12. Completely preserve the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the domains set forth in Appendix A to the complaint and preserve all evidence of any kind related to the content, data, software or accounts associated with such domains and computer hardware.

13. **IT IS FURTHER ORDERED** that in accordance with Rule 64 of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a), Plaintiff's request for an accounting of profits pursuant to 15 U.S.C. § 1117, and this Court's inherent equitable power to issue provisional

remedies ancillary to its authority to provide final equitable relief, Defendants and their agents, representatives, successors or assigns, and all persons acting in concert or in participation with any of them, and any banks, savings and loan associations, credit card companies, credit card processing agencies, merchant acquiring banks, financial institutions, or other companies or agencies that engage in the processing or transfer of money and/or real or personal property, who receive actual notice of this order by personal service or otherwise, are, without prior approval of the Court, temporarily restrained and enjoined from transferring, disposing or, or secreting any money, stocks, bonds, real or personal property, or other assets of Defendants or otherwise paying or transferring any money, stocks, bonds, real or personal property, or other assets to any of the Defendants, or into or out of any accounts associated with or utilized by any of the Defendants.

14. **IT IS FURTHER ORDERED** that Google may amend Appendix A to its complaint if it identifies other domains, or similar identifiers, used by Defendants in connection with the Malware Distribution Enterprise.

Security for Preliminary Injunction Order

IT IS FURTHER ORDERED that Google's submission of the \$75,000 bond to the Clerk made in connection with this Court's temporary restraining order satisfies the requirements this Court's preliminary injunction. See ECF 13 at 13. No additional bond is necessary.

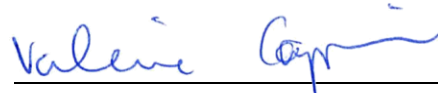
Status Report

IT IS FURTHER ORDERED, that Google shall file a status report on June 15, 2023.

So ordered.

SO ORDERED.

Date: May 5, 2023



United States District Judge

HON. VALERIE CAPRONI

UNITED STATES DISTRICT JUDGE